# Delaware State Police Issues Scam Alert Advisories

**Delaware** — The Delaware State Police is providing Scam Alert Advisories. This is a general alert that is applicable to the entire State of Delaware.

#### <u>Scammers ask for gift card payments</u>

Those who are victims of persistent scams involve a suspect posing as the IRS, FBI, law enforcement or some other agency. These scammers are usually asking for payments from victims to be made with Google play or other gift cards. The victims are instructed to go to a store and purchase gift cards. The victim is then told to scratch the coating off of the back of the purchased cards and read it over the phone. The victims then send it to the caller.

Purchasing a gift card for payment is NEVER legitimate and if anyone is asked to do that, they should report this to law enforcement. These suspects are very convincing and may have information on unsuspecting victims which makes them seem legitimate, but they are not.

# A relative has been arrested and jailed

Another scam is where a grandson (or other relatives) is in jail. The suspect claims to be a lawyer or someone from a police department in another state and the victim's relative had been in a collision where someone was injured and they need bail money. The caller requests money to be sent in cash via UPS/FedEx to another state.

## **Computer hacked**

Information regarding scams targeting the elderly. Elderly victims are tricked into believing that their computers had

been hacked. The victim then buys gift cards as payment for services to repair their computer problem(s).

#### Publisher's Clearing House Scam

Interestingly enough, a victim received a call from "Publisher's Clearing House" telling her that she had won the sweepstakes, but had to pay a percentage of her total winnings in order for her prize to be released. This victim having been duped already wised up and hung up on them.

# The Infamous Business Email Compromise (BEC)

This sophisticated scam targets businesses and individuals acting on wire transfer payments. The Delaware State Police New Castle County Financial Crimes is more likely to see this scammer's scheme because of the contingent of businesses in our area of responsibility. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts to conduct unlawful transfers of funds.

The scam may not always be associated with a request for the transfer of funds. A variation of the scam involves compromising legitimate business e-mail accounts and requesting Personal Information or Tax Information forms for employees.

#### <u>To summarize this scheme:</u>

A business (Usually real estate, non-profit, or accounting firms) receives an email from a regular customer under a spoofed email domain. For example, Firstname.Lastname@delaware.gov has been changed to Firstname.Lastname@delaware.edu. The suspect has already gained access to the business' email accounts and is expecting a wire transfer or payment that is supposed to go to the original recipient. The suspect poses as the legitimate customer and requests a wire transfer to a bank account. If the business doesn't catch the minor change money may be sent

to the suspect.

When the accounts are later remedied the victim realizes the mistaken money transfer. The attached Public Service Announcement checklist is for agencies to follow and how much this actually costs businesses.

To find out more click on the following link: PSA FBI

#### Added Forged Insurance Card

During Police Prosecution at the Justice of the Peace Court, a woman came in on a simple no proof insurance and speeding ticket. For the no proof insurance charge, she provided the trooper an intentionally altered insurance card. It was very obvious that is was fabricated and photocopied with the dates printed backward (expiration date was six months before the active date). The trooper subsequently called the insurance company and verified that the policy was canceled back in June of 2018 for lack of payment. She claimed she got it from her niece who owns the car and had no knowledge of the alteration. However, evidence proved she received a copy of the card. The information which included the image stated: "the card has been fixed." She and her niece were both arrested for Forgery 3rd Degree and Conspiracy.

Do not attempt to falsify any documents. See Criminal Code for Forgery. Click on the following link to find out more: <a href="Subsection 861 Felony Forgery">Subsection 861 Felony Forgery</a>

## Felony Forgery - Excerpt from the Delaware Criminal Code

A person is guilty of forgery when, intending to defraud, deceive or injure another person, or knowing that the person is facilitating a fraud or injury to be perpetrated by anyone, the person:

Alters any written instrument of another person without the other person's authority; or

Possesses a written instrument, knowing that it was made, completed or altered under circumstances constituting forgery.

Part of an issue of instruments issued by a government or a governmental instrumentality; or

A public record or an instrument filed or required to be filed in or with a public office or public servant; or

A written instrument officially issued or created by a public office, public servant or governmental instrumentality.

#### Red Flags, Best Practices, and Safety Tips

Scammers who operate by phone don't want to give you time to think about their pitch; they just want you to say "yes." But some are so sneaky that, even if you ask for more information, they seem happy to comply. They may direct you to a website or otherwise send information featuring "satisfied customers." These customers, known as shills, are likely as fake as their praise for the company. (Shill is a person who poses as a customer in order to decoy others into participating).

Here are a few red flags to help you spot telemarketing scams. If you hear a line that sounds like this, say "no, thank you," hang up, and file a complaint with the FTC:

- You've been specially selected (for this offer)
- You'll get a free bonus if you buy our product
- You've won one of five valuable prizes
- You've won big money in a foreign lottery
- This investment is low risk and provides a higher return than you can get anywhere else
- You have to make up your mind right away
- You trust me, right?
- You don't need to check our company with anyone
- We'll just put the shipping and handling charges on your credit card

#### **How Are People Fooled?**

Scammers use exaggerated — or even fake — prizes, products or services as bait. Some may call you, but others will use mail, texts, or ads to get you to call them for more details. Here are a few examples of "offers" you might get:

- Travel Packages. "Free" or "low cost" vacations can end up costing a bundle in hidden costs. Some of these vacations never take place, even after you've paid.
- Credit and loans. Advance fee loans, payday loans, protection, and offers to lower your credit card interest rates are very popular schemes, especially during a down economy.
- Sham or exaggerated business and investment opportunities. Promoters of these have made millions of dollars. Scammers rely on the fact that business and investing can be complicated and that most people don't research the investment.
- Charitable causes. Urgent requests for recent disaster relief efforts are especially common on the phone.
- High-stakes foreign lotteries. These pitches are against the law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail. What's more, you may never see a ticket.
- Extended car warranties. Scammers find out what kind of car you drive, and when you bought it so they can urge you to buy overpriced — or worthless — plans.
- "Free" trial offers. Some companies use free trials to sign you up for products —sometimes lots of products which can cost you lots of money because they bill you every month until you cancel.

# Why they're calling you...Why not?

Everyone's a potential target. Fraud isn't limited to race, ethnic background, gender, age, education, or income. That

said, some scams seem to concentrate in certain groups. For example, older people may be targeted because the caller assumes they may live alone, have a nest egg, or maybe more polite toward strangers.

Be Smart...How to Handle an Unexpected Sales Call. When you get a call from a telemarketer, ask yourself:

- Who's calling... and why? The law says telemarketers must tell you it's a sales call, the name of the seller and what they're selling before they make their pitch. If you don't hear this information, say "no thanks," and get off the phone.
- What's the hurry? Fast talkers who use high-pressure tactics could be hiding something. Take your time. Most legitimate businesses will give you time and written information about an offer before asking you to commit to a purchase.
- If it's free, why are they asking me to pay? Question fees you need to pay to redeem a prize or gift. Free is free. If you have to pay, it's a purchase not a prize or a gift.
- Why am I "confirming" my account information or giving it out? Some callers have your billing information before they call you. They're trying to get you to say "okay" so they can claim you approved a charge.
- What time is it? The law allows telemarketers to call only between 8 am and 9pm. A seller calling earlier or later is ignoring the law.
- Do I want more calls like this one? If you don't want a business to call you again, say so and register your phone number on the National Do Not Call Registry.

# If they call back, they're breaking the law.

Some Additional Suggestions

Resist pressure to make a decision immediately.

 Keep your credit card, checking account, or Social Security numbers to yourself.

Don't tell them to callers you don't know — even if they ask you to "confirm" this information. That's a trick.

- Don't pay for something just because you'll get a "free gift."
- Get all information in writing before you agree to buy.
- Check out a charity before you give. Ask how much of your donation actually goes to the charity. Ask the caller to send you written information so you can make an informed decision without being pressured or rushed into it.
- If the offer is an investment, check with your state securities regulator to see if the offer and the offeror are properly registered.
- Don't send cash by messenger, overnight mail, or money transfer. If you use cash or a money transfer — rather than a credit card — you may lose your right to dispute fraudulent charges. The money will be gone.
- Don't agree to any offer for which you have to pay a "registration" or "shipping" fee to get a prize or a gift.
- Research offers with your consumer protection agency or state Attorney General's office before you agree to send money.
- Beware of offers to "help" you recover money you have already lost. Callers that say they are law enforcement officers who will help you get your money back "for a fee" are scammers.
- Report any caller who is rude or abusive, even if you already sent them money. They'll want more. Call 1-877-FTC-HELP or visit ftc.gov/complaint.

# What to do about pre-recorded calls

If you answer the phone and hear a recorded message instead of

a live person, it's a robocall. Recorded messages that are trying to sell you something are generally illegal unless you have given the company written permission to call you.

#### If you get a robocall:

- Hang up the phone. Don't press 1 to speak to a live operator or any other key to take your number off the list. If you respond by pressing any number, it will probably just lead to more robocalls.
- Consider asking your phone company whether they charge for blocking phone numbers. Remember that telemarketers change Caller ID information easily and often, so it might not be worth paying a fee to block a number that will change.
- Report your experience to the FTC online or by calling 1-888-382-1222.

If you get phone service through the internet or cable, you might want to look into services that screen and block robocalls. Try doing an online search for "block robocalls."

# Tagged with: do not call, phone, scam, and telemarketing

Every year, thousands of people lose money to telephone scams — from a few dollars to their life savings. Scammers will say anything to cheat people out of money. Some seem very friendly — calling you by your first name, making small talk, and asking about your family. They may claim to work for a company you trust, or they may send mail.

If you get a call from someone you don't know who is trying to sell you something you hadn't planned to buy, say "No thanks." And, if they pressure you about giving up personal information — like your credit card or Social Security number — it's likely a scam. Hang up and report it to the Federal Trade Commission.

Each year seniors lose millions of dollars to phone scams keep

the following in mind so you don't become a victim

- If you get a call saying you're a winner don't pay any money to collect supposed sweepstakes winnings. Legitimate operations won't require you to pay to collect your winnings.
- It's against federal law to play a foreign lottery so if you get a call it is likely a scam.
- Never wire money to anyone with whom you are not familiar.
- Never provide anyone with personal information such as bank accounts, pin numbers or Social Security numbers.
- Check any unfamiliar area codes before returning calls.
- Be aware that there are many 3-digit area codes that connect callers to international telephone numbers especially 876.
- If you do not have Caller ID, consider adding it to your phone service. Caller ID allows you to add a Call Intercept feature that screens calls and offers the option to reject suspicious international calls.
- If you do not make international calls, ask your telephone provider to block outgoing international calls.
- Contact your local authorities to report a phone scam;
  however, the smartest thing to do is hang up the phone.

This past year the Delaware State Police have been made aware of unsolicited phone calls being received by members of the community, from individuals claiming to be with the IRS. The scam involves a person calling claiming the victim owes money to the IRS and it must be paid promptly. If the victim refuses, they are threatened with arrest, deportation, or suspension of their driver's license, amongst other things. In the most recent phone calls, the individual requests the victim send money in the form of an iTunes card.

#### Note that the IRS will never:

Call to demand immediate payment, nor will the agency call about taxes owed without first having mailed you a bill.

Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.

Require you to use a specific payment method for your taxes, such as a prepaid debit card.

Ask for credit or debit card numbers over the phone.

Threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.

\*\*This information was provided through the IRS website located at <a href="http://www.irs.gov/uac/Tax-Scams-Consumer-Alerts">http://www.irs.gov/uac/Tax-Scams-Consumer-Alerts</a>

Many of these scams are difficult to investigate. They will target persons of all age groups. The Delaware State Police is asking citizens to remember the tips previously mentioned in order to not become a victim of one of these scam artists.

If you suspect you have been a victim of this scam, please contact your local law enforcement agency. Information may also be provided by calling Delaware crime stoppers at 1-800-TIP-3333 or via the internet at <a href="http://www.delaware.crimestoppersweb.com">http://www.delaware.crimestoppersweb.com</a>

You can follow the Delaware State Police by clicking on:

Delaware State Police Official Web Site

<u>Facebook</u>

<u>Twitter</u>

<u>Nextdoor</u>

Please tell us how we're doing via our <u>Citizen Satisfaction</u> <u>Survey</u>.

# Presented by the Director of Public Information, Sergeant Richard Bratz

Released: 071019 1713

-End-